Setup and Configure

WhyRoute2.

WhyRoute. Monitoring, Secure and easy setup with support.

The WhyRoute product provides an all in one monitoring system on one machine and contains many exclusive features such as:

- Supports RDP, VNC and SSH – Allowing you to connect to multiple devices from WhyRoute
- Network IP Scanner – Identify free IP addresses for installation and rogue devices and find your devices on the network
- Open Ports Scan – Test what ports are open for troubleshooting and security reasons
- Ubiquiti Unifi Controller – Allowing you to control your Ubiquiti Unifi Wireless systems
- Network Monitoring – Monitors your network so you can proactively respond to devices going down or having any other issues. Cybersecurity features with perimeter scans.
- OpenVPN – Allow Remote VPN, Switch on and open ports
- DDNS Client – Works with DynDNS, NoIP and many others.
- Remote Access – Via our online portal you can access in your system from anywhere in the world.
- First months monitoring free.
- Based on linux and hardened.

The goal of WhyRoute is to make life for customers so much easier by helping customers proactively deal with issues on their network from anywhere in the world, this is a revolutionary toolkit that can be deployed in homes and businesses.

SUPPORT CONTACT:
http://www.whyroute.com/
support@whyroute.com

We have done most of the setup for you to simplify the setup of WhyRoute2.

Simply plug it into your network and power and switch on.

Please note: We have purposefully not enabled POE on the device in case there is an issue with POE on the switch.

I	–	Initial Setup
II	-	Move the device into another group in the portal
III	-	Remote into another machine using RDP, VNC or SSH
IV	-	Setup Monitoring
V	-	Setup Unifi Controller
VI	-	Setup VPN Service
VII	-	Enable DDNS Client
VIII	-	Scan your network for IPs
IX	-	Scan an IP/DNS Address for open ports
X	-	Access WhyRoute2 from the network using SSH
XI	-	Setup Website Monitoring

I Initial Setup

1. Plug into power and network
2. Switch on
3. Go to https://access.whyroute.com and login
4. Click on your newly added device
5. Click on Desktop
6. Click Connect
7. Log into your device using the password of in2RPi2019
   If you would like to change this password do the following:
   a. Click the start menu in the top left-hand corner
   b. Go to Preferences
   c. WhyRoute2 Configuration
   d. Click Change password
   e. Enter your new password and click OK
   f. Click OK
8. You can also use the terminal on Mesh to reboot the device, ping, telnet etc
   If you want to setup a static IP address do the following:
   a. Right Click on the Arrows in the top right hand corner
   b. Click on Wireless & Wired Network Settings
   c. Choose eth0 from the Interfaces drop down list
   d. Fill in the details as laid out
   e. Click Apply
   f. Click Close

II To move the device into another group in the Mesh portal

1. Click Add Device in the portal
2. Drop down to Linux Install
3. Copy all the text
4. Open lxterminal
5. Type in sudo ./meshinstall.sh uninstall &&
6. Paste in the text copied above and then hit enter
7. The session will disconnect and the machine will show up in a new group.
   a. Alternatively you could make up the plan in a text editor and make up the command then paste that in

III To Remote into another machine using RDP, VNC or SSH

1. Open Remmina from the desktop
2. Choose the protocol you want to use
3. Type in the address for the machine
4. Click Connect

IV To Setup Monitoring

1. Click on the WhyRoute2 Admin Shortcut on the Desktop
2. Click on the Domotz Network Monitoring
3. Log in or setup a new account

V To Setup Unifi Controller

1. Click on Enable Unifi Controller
2. Click Execute in Terminal
3. Once the terminal has closed Click on the WhyRoute2 Admin Shortcut on the Desktop
4. Click on Unifi Controller
5. Run the setup

VI To Setup VPN

1. Click on Enable OpenVPN
2. Click Execute in Terminal
3. Once the terminal closes open port 1194 UDP on your firewall and point it to your device
4. Click on the WhyRoute2 Admin Shortcut on the Desktop
5. Click on OpenVPN and login using Username: whyvpn Password: in2OVPN4WRpia1021
6. Click on Configs
7. Change “SERVERNAME” to your external IP Address for the Operating system you will use
8. Wait until the icon on the top right of the text box changes to green
9. Click on Configurations
10. Put in the username default-ovpn, password in2WRovpn4WRpia1021 and select your operating system
    If you would like to change the password or add new users do the following:
    a. Click on OpenVPN Users
    b. To add a new user click + and fill in the requested details
    c. To change any passwords click on the password, put in a new password and click the tick
11. Click Get configuration files
12. Once downloaded open with OpenVPN on your machine and connect using the details above.

VII To Enable DDNS Client

1. Click on Dyndns
2. Click on Execute in terminal
3. Once the terminal comes up fill in the details as prompted

VIII To Scan your network for IPs

1. Click on Zenmap
2. Click OK
3. In target enter the range you want to scan e.g. 192.168.1.1-100
4. Click Scan

IX To Scan a device on your network or externally for open ports

1. Click on Zenmap
2. Click OK
3. In the target enter the device IP or address you want to scan
4. Choose your required profile
5. Click Scan

X Access WhyRoute2 from the network using SSH

1. Open your SSH client
2. Type in the IP address of WhyRoute2 and connect
3. Enter the username pi and password in2RPi2019

XI Setup Website Monitoring

1. Click on Enable Webmon
2. Click Execute in Terminal
3. Once the terminal has closed Click on the WhyRoute2 Admin Shortcut on the Desktop
4. Click on Webmon Administration
5. Login with monadmin (it will show up in the drop down list) password is in2PSM4WRa
6. Click on Servers
7. Click on Add new
8. Fill in requested details

    Tip: If you want to Monitor a website for changes choose a piece of string that can be found in the HTML source and put it into the Search String/Pattern Box